Consumer Notice
Phishing

March 14, 2013

Phishing may be a new term to you, but it describes a term that is widely known and used by online criminals and scammers. What is phishing? Phishing is the use of e-mail messages, websites and even telephone calls that are designed to trick you into revealing personal information in order to steal your identity and/or your money.

Phishing can be accomplished in a variety of methods. This can be done by having malicious software that is contained in the code of an e-mail message or a website address, which is loaded into your computer for the sole purpose of stealing your personal identifying information that may be stored in your computer.

The scammers may also attempt to convince you through an e-mail message, downloading software from a website, or through direct telephone contact to provide your personal identifying information by using false pretenses.

A phishing e-mail may contain obvious spelling and grammatical errors and it may also provide links to a website, which may be unfamiliar to you. Some of the e-mail may also use threats stating that your account is about to be closed and ask for you to confirm your password information.

Additionally, online criminals and scammers may use graphics in an e-mail or on a website link which appear to be connected to a legitimate company name or web site; however, often times, these will link you to phony websites. They may also use web addresses that resemble well-known companies, but they will alter the web address just enough to give the appearance it is a legitimate website.

Finally, if anyone contacts you stating they are a representative of a financial institution and they need your account number and/or password due to a problem with your account, do not provide the caller with this information. Financial institutions have your account number information readily available and would not have a need to request such information from you.

If you receive a questionable phone call where the caller represents that he or she is a financial institution calling for your account information, take down as much information as possible regarding the call and report it to your local law enforcement officials. Remember not to fall for these scams by providing your personal identifying information.

Any suspicious e-mail phishing attempts can be reported to the Anti-Phishing Working Group by forwarding the suspicious e-mail to them at reportphishing@apwg.org.

The following links to the FDIC, National Credit Union Administration (NCUA) and the Tennessee Attorney General and Division of Consumer Affairs provide more information on phishing for your reference:

FDIC: http://www.fdic.gov/consumers/consumer/alerts/phishing.html
NCUA: http://www.ncua.gov/Resources/Documents/LCU2004-12.pdf
Tennessee Attorney General: http://www.tn.gov/attorneygeneral/press/2005/story/pr3.pdf
Division of Consumer Affairs: https://news.tn.gov/node/9927

If you become a victim of a phishing scam where you mistakenly provide your personal identifying information, contact your financial institution as soon as possible to make them aware. This will allow the financial institution to take certain steps to lessen or limit any damage to your personal account.

You will also want to report this to local law enforcement officials.

If you want to notify the Department of Financial Institutions about any complaints you have regarding phishing activities, you can report those instances to:

Consumer Resources
Tennessee Department of Financial Institutions
414 Union Street, Suite 1000
Nashville, TN 37219
800-778-4215 toll-free
615-253-2023 local
615-253-7794 fax
www.tdfi.gov/tdfi